advertisement

BUSINESS MAR 2 2018, 7:21 PM ET

The hidden dangers of buying virtual currency go beyond a simple hack

by **HERB WEISBAUM**

SHARE

That cryptocurrency you just bought is as vulnerable to hackers as your smartphone or any other digital device, security experts are warning.

Virtual — and increasingly popular — currencies like bitcoin, Ethereum, and Litecoin are unregulated and volatile, making them not just a high-risk investment, but criminals can break into crypto exchanges, drain crypto wallets and infect individual computers with malware that steals cryptocurrency.

Most buyers believe virtual currencies are a secure way of making payments — without really understanding how they work. Dado Ruvic / Reuters

Still, most buyers believe these currencies provide a safe and secure way of making payments — even though most people don't have a clue as to how they work.

A recent report from ThreatMetrix cautions: "Cryptocurrency has moved from being the playground of the criminal underworld to be a prime target for attacks on legitimate transactions."

Related: What is Bitcoin? And should you invest in it?

A new report from Ernst & Young provides some of the first hard numbers on this new crime spree. EY analysts looked at 372 initial coin offerings that occurred between 2015 and 2017 and found that more than 10 percent of the funds — as much as $1.5 million a month — were stolen.

"Cryptocurrency transactions are typically not reversible," said Paul Brody, EY's global innovation blockchain leader. "Blockchains are decentralized payment systems, so there is no central power that can reverse a transaction that wasn't right." The EY report warns that these crypto-attacks are becoming more frequent. In many cases, the hackers are using a well-tested tool — phishing email — to gain access to digital currency storage systems.

> **“Even large companies have been defrauded. It happens to everybody, even people who think they are experts.”**

“And it's not just individuals,” Brody told NBC News. “We've worked with large companies that have been defrauded — multi-million dollar losses — through phishing. It happens to everybody, even people who think they’re experts.”

An analysis of the most common cybercrimes involving Ethereum by Chainalysis, a provider of risk management software for virtual currencies, found that phishing is currently creating the most losses. Phishing is responsible for more than 50 percent of all cybercrime revenue — estimated at more than $225 million — generated from Ethereum in 2017, the company reported in a blog post last year.

Criminals follow the money

Cyber thieves have watched bitcoin’s meteoric rise in value and decided it’s time to cash in. At least four advanced criminal groups that used malware to attack bank accounts have shifted their focus to hack bitcoin and cryptocurrency exchanges, Avivah Litan, a vice president and distinguished analyst at Gartner Research, told NBC News.

“It’s because that’s where the money is,” Litan said. “Consumers are investing in bitcoin and the criminals are following the retail trends. But the average consumer doesn’t realize the risk.”

Related: 600 powerful computers stolen in Iceland Bitcoin heist

In January, hackers stole about $530 million from Coincheck, the leading bitcoin and cryptocurrency exchange in Asia. This is believed to be the largest crypto heist to date. (Coincheck has promised to return $425 million of the virtual money it lost, Reuters reported.)

Litan predicts more of these attacks. In a recent blog post she says crypto hackers are active and ready to attack U.S., Japanese and UK cryptocurrency exchange customers.

Bitcoin-hijacking malware targets cryptoexchanges

A new report from IBM’s X-Force research group provides details about the TrickBot malware (one of the top six banking Trojans of 2017) and how criminals have modified it to target cryptocurrency exchanges by redirecting

bitcoin to their wallets during a trade or purchase.

IBM calls the modified TrickBot Trojan “a triple-threat” because it captures the victim’s exchange login credentials, snags their crypto wallet information and steals their credit card information.

“Since TrickBot grabs the victim's login credentials to their cryptocurrency exchange, the criminals can go back in, log in as this person and steal the rest of the bitcoins they may already have in their wallet, or purchase more bitcoin because they’ve also stolen their credit card information,” said John Kuhn, senior threat researcher with IBM X-force. “All sorts of bad things can happen, if you get infected with this particular piece of malware.”

Some credit cards have banned crypto purchases

About 18 percent of bitcoin investors pay with a credit card, according to a survey conducted by LendEDU in December. And nearly one-quarter of them could not pay off their balance after making the purchase.

Faced with a growing risk from these cryptocurrency purchases — including fraudulent transactions, disputed charges from cardholders burned by a crypto scam and the inability for some to pay off these large purchases — several of America’s largest banks have decided to ban crypto purchases.

CNBC reported in early February that JPMorgan Chase, Bank of America, and Citigroup will no longer allow cardholders to buy cryptocurrency. A spokesman for JPMorgan Chase told CNBC the new policy was “due to the volatility and risk involved.” Citibank said it would continue to review its policy as this market evolves.

The Wall Street Journal reported in late January that Capital One will not allow cardholders to buy cryptocurrencies “due to the limited mainstream acceptance and the elevated risks of fraud, loss and volatility.”

Discover told NBC News it does not allow cryptocurrency purchases with the Discover card because it is “based largely on a lack of transparency, underwriting risks and money laundering concerns.”

Steve Kenneally, senior vice president for payments and cybersecurity policy at the American Bankers Association, told NBC News that some banks have moved to stop credit card purchases of cryptocurrencies because “purchasing them is speculative and risky,” as demonstrated by their recent volatility in value.

“There is a risk the borrower will be unable to repay the loan, if the value of the cryptocurrency falls dramatically after the purchase,” Kenneally said in an email. “There is also an elevated risk for fraud and concerns about the lack of transparency around purchases of cryptocurrencies.”

What about government regulation? Don’t count on it.

“Regulators in the U.S. and Canada are taking a light-touch approach because they don’t want to hurt the innovation that’s occurring around blockchain, the infrastructure behind the cryptocurrency,” said Kristina Yee, senior analyst with the Aite Group. “But other places, like China, are very concerned about the use of cryptocurrencies for hiding money and getting it out of the country, so there’s a clampdown on cryptocurrency there.”

How to protect yourself

Cryptocurrency transactions are final. There’s no anti-fraud guarantee from a financial institution and no reversing the charges, if there’s a problem. And while blockchain technology will show you which computer snagged your money, it’s virtually impossible to identify or prosecute the criminals who robbed you.

“We whole-heartedly believe that cryptocurrency is going to be a major focus for this year and probably a few years to come,” IBM X-Force researcher John Kuhn told NBC News. “The security and everything involved in cryptocurrency really isn't up to speed to normal financial institution levels, so it’s kind of a soft and easy target.”

That means if you dabble in digital currency, you need to protect yourself. Digital security experts advise:

- Stick to well-known exchanges, such as Coinbase, the leading U.S. marketplace for buying major cryptocurrencies, for any transactions. You want one that offers two-factor or multifactor authentication.
- Don’t store a lot of digital currency online. You can keep a little in an exchange, but have the rest in a physical wallet.
- Keep your operating system and security software up-to-date with the latest updates and patches. Set your devices to apply updates automatically.
- Be on guard for phishing emails. No matter how urgent or ominous the message, never provide sensitive information when requested this way. Anyone who needs your log-in or account information already has it.

- Practice general computer security hygiene every single day to reduce your risk of downloading malware that targets crypto transactions. That means: If you didn't expect that email, don't click on the links or open any attachments.

Herb Weisbaum is The ConsumerMan. Follow him on Facebook and Twitter or visit The ConsumerMan website.

HERB WEISBAUM

TOPICS BUSINESS, BUSINESS NEWS

FIRST PUBLISHED MAR 2 2018, 2:52 PM ET

NEXT STORY Disney names longtime executive James Pitaro as new ESPN president

More to Explore Sponsored Links by Taboola

Cheap Flights - Compare Rates and Save!
Lastmin-Flights

One of The Cheapest Ways to Get a Flight Ticket
LaseTrips.com

The New Travel Site That Just Kills it!
Save70.com

Book Flights Last Minute For Huge Savings!
Lastmin-Flights

Cheap All-Inclusive Cruises
Cruises-Shop

Find cheap Cruises
Cruise-Compare.com

SPONSORED CONTENT **MORE FROM NBC NEWS**

Want To Be Own Boss In 2017? Start An Online Business In You…
Project Ignite

Flight Prices So Cheap That Even Babies Will Fly Save70.com

New Site Finds the Cheapest Flights in Seconds! FlightFinder

Lankford: 'The problem is not owning an AR-15' NBC News

Flight Prices You're Not Allowed to See! Save70.com

Texas school will suspend students who protest gun rights

'Three Billboards' is for people who want to feel better about their raci…

Citigroup refunding $330 million to customers after overcharging interest

It’s official, Switzerland is fast becoming a 'Crypto-Nation'

Chuck Todd: Boycotts have shown how poorly the NRA has handled the…

Promoted Links by Taboola